

QUELLE GOUVERNANCE MONDIALE DE L'INTERNET APRES L'AFFAIRE SNOWDEN ?

BERNARD BENHAMOU

Enseignant à l'Université Paris I – Panthéon Sorbonne sur la gouvernance de l'Internet et
ancien délégué interministériel aux usages de l'Internet et conseiller de la délégation
française au Sommet des Nations Unies sur la société de l'Information

En l'espace de quelques années, l'Internet est devenu l'une des infrastructures les plus cruciales de nos sociétés tant sur le plan politique et social que sur le plan économique. Dans le même temps, l'architecture et la gouvernance du réseau sont devenues l'enjeu de conflits entre acteurs industriels mais aussi de tensions internationales liées à la tentation de contrôle politique du réseau. Les révélations d'Edward Snowden sur l'étendue des programmes de surveillance de la NSA, si elles ont suscité de légitimes inquiétudes auprès des citoyens, pourraient aussi avoir d'importantes conséquences industrielles pour l'ensemble des acteurs de l'Internet. En effet, en remettant en cause la confidentialité des échanges sur Internet, les pratiques de la NSA ont modifié profondément la perception de la sécurité et de la vie privée sur Internet. L'affaire Snowden pourrait aussi provoquer des changements majeurs dans l'architecture et dans la gouvernance mondiale de l'Internet¹.

GOUVERNANCE DES INFRASTRUCTURES OU GOUVERNANCE DES TECHNOLOGIES ?

La gouvernance de l'Internet a souvent été décrite comme la concertation des acteurs impliqués dans la gestion technique et politique du réseau mondial². Cependant, depuis la création de l'organisation chargée de la gestion des noms de domaines sur Internet, c'est essentiellement

¹ *Politique et architecture de l'Internet* (B. Benhamou, Revue Esprit 5/2006)

<http://www.netgouvernance.org/ArchitectureEsprit.pdf>

² « Par "gouvernance de l'Internet" il faut entendre l'élaboration et l'application par les États, le secteur privé et la société civile, dans le cadre de leurs rôles respectifs, de principes, normes, règles, procédures de prise de décisions et programmes communs propres à modérer l'évolution et l'utilisation de l'Internet » (Extrait du rapport du Groupe de travail sur la Gouvernance de l'Internet des Nations unies, juin 2005) <http://www.wgig.org/docs/WGIGREPORT.pdf>

L'organisation des infrastructures critiques de l'Internet qui a donné lieu à des tensions internationales³. C'est le cas de l'ICANN⁴, l'association de droit californien créée par l'administration Clinton en 1998 pour gérer les noms de domaine sur Internet, qui est rapidement devenue l'objet de tensions entre les États. En effet, les pouvoirs d'organisation de la cartographie mondiale de l'Internet conférés à l'ICANN incluent des prérogatives de souveraineté dont les États ne pouvaient être privés dans la durée en particulier pour la gestion des extensions dédiées aux pays (.fr, .de, .ru, etc.). L'ICANN a en effet depuis sa création prôné un statu quo favorable aux États-Unis. La structure qui au sein de l'ICANN est chargée de valider l'ensemble des extensions de l'Internet (IANA) est jusqu'à ce jour liée par un contrat avec le Département du Commerce des États-Unis. De plus, le rôle politique mais aussi le fonctionnement économique de l'ICANN font encore l'objet de nombreuses controverses. C'est en partie pour tenter de faire évoluer le mode de gouvernance des noms de domaine que les Nations Unies ont organisé le Sommet Mondial sur la Société de l'Information (SMSI 2003-2005). Le texte adopté à l'issue de sommet, l'Agenda de Tunis, n'a cependant pas permis de faire évoluer le statu quo. Récemment encore, lors de la Conférence mondiale sur les télécommunications (WCIT 2012) de nombreux pays émergents et en particulier la Chine, la Russie et les Émirats arabes unis, ont souhaité que la gouvernance de l'Internet échappe aux seuls États-Unis et soit placée sous le contrôle exclusif des gouvernements. L'Union européenne avait alors refusé de signer cette proposition qui aurait pu avoir des conséquences politiques et économiques imprévisibles en raison de la « fragmentation » de l'Internet en une série d'îlots. Ce n'est qu'à l'issue des révélations d'Edward Snowden sur les programmes de surveillance de la NSA que les autorités américaines ont proposé de remettre en cause ce contrat avec l'ICANN⁵.

LA CONFIDENTIALITE CLE DE VOUTE DE L'INTERNET

La montée en puissance des réseaux sociaux et la montée en puissance de l'Internet mobile ont en effet créé les conditions d'une collecte massive des données sur les internautes. Ainsi, la découverte de l'étendue des données collectées par la NSA auprès des géants de l'Internet via le programme PRISM a constitué un « séisme » pour les opinions publiques et aussi pour l'ensemble des acteurs de l'Internet. Ceux-ci ont en effet découvert que leurs infrastructures étaient devenues « transparentes » pour les agences gouvernementales. Pour la première fois depuis la création de l'Internet, ces révélations ont créé les conditions d'un « schisme » entre les industriels de l'Internet et le gouvernement américain. Ainsi, les géants de la Silicon Valley ont fait savoir à

³ *Internet et souveraineté : la gouvernance de la Société de l'Information* (B. Benhamou et L. Sorbier, Politique Étrangère - 2006) http://ifri.org/files/politique_etrangere/PE_3_2006_Benhamou.pdf

⁴ L'ICANN (Internet Corporation for Assigned Names and Numbers) assure la gestion du DNS (Domain Name System) qui constitue « l'annuaire mondial » des ressources sur Internet et permet de convertir des adresses IP numériques en noms de domaine intelligibles.

⁵ *U.S. to Cede Its Oversight of Addresses on Internet* (New York Times, 14/03/2014) <http://nyti.ms/1pib1Xg>

Barack Obama à quel point la NSA pouvait remettre en cause la clef de voûte de l'Internet : la confiance de ses usagers⁶. Mark Zuckerberg le PDG de Facebook déclarait même récemment : « *Le gouvernement américain est devenu une menace pour l'Internet...*⁷ »

Les nouveaux enjeux de la gouvernance de l'Internet sont en effet liés aux technologies qui permettent de préserver la confidentialité et de protéger la vie privée des usagers. Il est à noter qu'aucun des programmes de surveillance mis en place par la NSA ne reposait sur les fonctions ou prérogatives de l'ICANN qui excluent les questions liées à la sécurité des contenus et la protection de la vie privée sur Internet. Ainsi, plus que l'organisation générale des noms de domaine sur Internet, ce sont les normes et standards qui assurent le bon fonctionnement du réseau qui ont été au cœur des actions de la NSA.

DES LIBERTES PUBLIQUES AUX CONSEQUENCES ECONOMIQUES

Les instances qui élaborent ces normes et standards de l'Internet, sont les véritables « assemblées constituantes » du réseau. Ces instances étaient déjà le théâtre de l'affrontement entre acteurs industriels, elles sont devenues les nouveaux lieux de l'influence des agences gouvernementales de sécurité. C'est le cas de l'IETF (Internet Engineering Task Force), le collège mondial des ingénieurs du réseau, qui valide les technologies qui seront utilisées à l'échelle mondiale pour faire fonctionner l'Internet. Pour faciliter la mise en place de ses programmes de surveillance, la NSA a souhaité être en mesure d'accéder à l'ensemble des échanges cryptés sur Internet. C'est l'objet du programme Bullrun⁸ de la NSA dont les ingénieurs ont volontairement altéré la confidentialité des échanges en introduisant dans les algorithmes de chiffrement des « portes dérobées » ou « backdoors⁹ » qui permettaient de décrypter les messages. S'il est moins connu du grand public que le programme PRISM, le programme Bullrun a eu des répercussions majeures sur l'ensemble des acteurs économiques soucieux de protéger leurs données sensibles. L'équipementier Cisco a ainsi souffert des « répliques » liées à ce volet de l'affaire Snowden en particulier dans les pays émergents qui ont remis en cause de nombreux contrats en raison des risques de surveillance qu'aurait pu engendrer l'acquisition de matériels américains¹⁰.

Pour être en mesure de rétablir la confiance sur Internet, les communautés d'ingénieurs souhaitent désormais se réapproprier un réseau dont les bases mêmes ont été réorientées pour satisfaire les intérêts des agences de sécurité gouvernementale. À l'issue des révélations d'Edward

⁶ *Tech executives to Obama: NSA spying revelations are hurting business* (Washington Post 17/12/2013) <http://wapo.st/1kfMSAZ>

⁷ Editorial de Mark Zuckerberg posté sur Facebook le 13/03/2014 <http://on.fb.me/1nVf2Cc>

⁸ <http://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying>

⁹ *The internet after Snowden : New threat model army* (The Economist, 11/11/2013) <http://econ.st/1r5U71J>

¹⁰ *Cisco cites emerging markets backlash on NSA leaks for sales slump* (Financial Times, 13/11/2013) <http://on.ft.com/1eulgWJ>

Snowden, Vinton Cerf, le créateur des protocoles fondamentaux de l'Internet et président fondateur de l'ICANN, reconnaissait qu'il aurait été nécessaire d'intégrer au cœur même de ces protocoles des dispositifs de cryptage¹¹. Cette préoccupation a aussi été au cœur de la proposition de la chancelière allemande Angela Merkel de protéger les données personnelles des citoyens en modifiant l'architecture des services qui recueillent ces données en Europe¹².

Le besoin de préserver la vie privée pourrait en effet s'accroître encore en raison des évolutions technologiques de l'Internet vers un « Internet des Objets » qui connectera bientôt plusieurs milliards d'objets dans l'environnement des usagers. Ces objets connectés seront utilisés dans le domaine de la santé, de la maîtrise de l'énergie ou encore des transports. Ils seront dotés de nombreux capteurs et pourraient, là encore, être à l'origine de nouvelles formes de surveillance. Les informations issues de ces objets connectés devront donc être à la fois confidentielles et sécurisées pour leurs usagers¹³.

DES PRINCIPES AUX ACTIONS INTERNATIONALES

Plutôt que d'impliquer les agences de sécurité dans la conception des normes et standards de l'Internet, les États doivent désormais éviter que ces normes soient mises au service d'un seul État ou d'un groupe d'États et remettent en cause les principes du fonctionnement de l'Internet pour l'ensemble de ses usagers. Comme l'a rappelé le rapport du groupe d'experts sur la cybersécurité remis à la Maison Blanche¹⁴, il convient de rétablir un nouvel équilibre entre les contraintes de sécurité et le fonctionnement de nos démocraties.

La situation nouvelle créée par la mise en place des programmes de surveillance de masse sur Internet par les États-Unis crée une opportunité pour l'Europe de devenir l'artisan d'un accord transatlantique qui établirait les principes fondamentaux du développement de l'Internet dans les démocraties. Dans cette perspective, l'inventeur du web, le britannique Tim Berners-Lee, a déjà réclamé que soit créée une Constitution mondiale pour l'Internet¹⁵. Cet « Internet Bill of Rights » ou cette « Magna Carta » pourrait placer les principes fondamentaux de l'Internet au-dessus des lois nationales afin que les États ne puissent unilatéralement modifier l'Internet à des fins

¹¹ <http://www.scientificamerican.com/article/fact-fiction-encryption-prevents-digital-eavesdropping/>

¹² *Data protection: Angela Merkel proposes Europe network* (BBC 15/2/2014) <http://www.bbc.com/news/world-europe-26210053>

¹³ *Les mutations économiques, sociales et politiques de l'Internet des objets* (B. Benhamou, Cahiers Documentation Française 12/2012) <http://www.netgouvernance.org/IOT%20Cahiers%20DOC%20FRANCAISE.PDF>

¹⁴ *Liberty and Security in a Changing World* (President's Review Group on Intelligence and Communications Technologies, 12/12/2013) http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

¹⁵ *An online Magna Carta: Berners-Lee calls for bill of rights for web* (The Guardian, 12/03/2014) <http://www.theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web>

économiques ou politiques. C'est ce principe qu'avait aussi évoqué Viktor Mayer-Schoenberger, de la Harvard Kennedy School, dans son étude de la proposition européenne lors du Sommet des Nations unies. Dans cette étude, au titre évocateur « Jefferson Rebuffed¹⁶ » (Jefferson repoussé), il notait qu'un « moment constitutionnel » avait été manqué par les États-Unis en 2005 en repoussant la proposition européenne qui prévoyait d'inscrire dans les textes internationaux les trois principes fondamentaux liés à l'architecture de l'Internet (l'ouverture, l'interopérabilité et la neutralité de l'Internet). À ces trois principes, il conviendrait aujourd'hui d'en ajouter un quatrième qui interdirait aux États de prendre des mesures à même de porter atteinte au fonctionnement du réseau pour l'ensemble de ses utilisateurs. La création d'un accord transatlantique permettrait aussi de fonder une opposabilité juridique internationale aux actions technologiques des États qui mettraient en péril le bon fonctionnement et la sécurité du réseau. Il pourrait ainsi dans un second temps être élargi à d'autres régimes démocratiques afin de veiller à ce que de nouvelles crises liées à la confiance ne puissent fragiliser l'architecture mondiale de l'Internet.

¹⁶ *Jefferson Rebuffed - The United States and the Future of Internet Governance* - Viktor Mayer-Schoenberger et Malte Ziewitz – John F. Kennedy School of Government, Harvard University (mai 2006) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=902374